National security, legal readiness, and U.S. engagement for international dual-use technology companies

By Scott Nuzum, Esq., Wiley

OCTOBER 3, 2025

The term "dual-use technology" refers to innovation with both civilian and military applications. For decades, the epicenter of this innovation was unmistakably American. From DARPA to Skunkworks to Los Alamos, U.S. institutions produced breakthroughs that reshaped warfighting and daily life alike. GPS, semiconductors, stealth technologies, and countless other technologies illustrate how American ingenuity served as a force multiplier for U.S. economic growth, hard power, and global influence.

Propelled by the rise of generative AI tools, regional reindustrialization, and battlefield testing in active conflict zones, some of the most consequential dual-use technology companies are being built beyond U.S. shores.

That monopoly, however, has given way to a far more distributed global ecosystem. Over the past 30 years, as the world has become increasingly multipolar and the post-WWII order more fragile, dual-use innovation has flourished well beyond U.S. borders.

Propelled by the rise of generative AI tools, regional reindustrialization, and battlefield testing in active conflict zones, some of the most consequential dual-use technology companies are being built beyond U.S. shores. Some of these innovations are being developed in countries aligned with U.S. interests, in places like Cologne, Canberra, and Kyiv. Others are emerging in jurisdictions where alignment with U.S. interests is uncertain, if not directly opposed.

This diffusion of innovative capacity has coincided with a broader policy turn toward nationalistic industrial strategies. Across the globe, governments increasingly emphasize sovereign alignment, industrial resilience, and state-led technology initiatives as central to security.

In the United States, new trade measures, evolving compliance frameworks, and shifting geopolitical and regulatory dynamics have raised the threshold for foreign participation in U.S. federal contracting, investment, and cross-border collaboration. At its core, this approach reflects a doctrine of "national security through industrial capacity," in which access to U.S. markets and partnerships is increasingly conditioned on supply chain resilience, technological sovereignty, and alignment with U.S. national security priorities.

Even with these shifts, the United States remains uniquely attractive. It combines the world's deepest pool of private capital, unparalleled depth in venture and strategic investment, predictable intellectual property enforcement, a dense concentration of talent, and an annual federal procurement budget exceeding $750 billion.

In today's global technology order, national security is no longer a siloed legal discipline; it is the lens through which opportunity, access, and trust are evaluated.

No other market offers the same scale, legal stability, and opportunity. Yet accessing this market in 2025 means navigating a legal and policy landscape where national security concerns inform virtually every transaction. The Defense Production Act, CHIPS Act, and other industrial planning authorities laid important groundwork, but today's environment goes further, emphasizing supply-chain control and technology flows as essential instruments of national policy.

For foreign companies, success in the United States requires more than technical excellence; it demands a deliberate legal, structural, and commercial strategy that anticipates and addresses U.S. security concerns. Those able to meet these requirements can unlock opportunities that are difficult to replicate elsewhere: entry into procurement programs, partnerships with strategic investors, and long-term collaborations at the center of the world's most dynamic innovation ecosystem.

Legal filters for trust and access

So, what does such a strategy require? At its core, it hinges on demonstrating credible alignment with U.S. national interests. This alignment is evaluated through a national security risk lens that is increasingly multi-dimensional, and includes the following factors:

- **Foreign Ownership, Control, or Influence (FOCI):** FOCI mitigation has become a standard due diligence inquiry for any company seeking to do classified work or access Controlled Unclassified Information (CUI). It is a protracted process that can take years to complete, requiring formal agreements with the U.S. government (such as Special Security Agreements or Proxy Boards) and the implementation of governance controls, such as ring-fencing and information firewalls.
- **Export control**: Export control regimes (ITAR and EAR) are being enforced more aggressively in light of recent geopolitical tensions. For example, a company developing autonomous maritime drones for environmental mapping may still be captured under dual-use rules if the technology can be adapted for naval surveillance or mine detection.
- **Committee on Foreign Investment in the United States (CFIUS)**: CFIUS risk awareness has migrated from M&A transactions into strategic contracting. U.S. government counterparties (and primes) increasingly evaluate whether subcontractors or licensors pose future foreign influence risks that could trigger CFIUS review in the event of a downstream capital event.
- **'Critical Technologies' definitions**: The definition of "critical technologies" is expanding, with some agencies adopting internal lists of sensitive technologies that go well beyond the formal export control schedules. Participation in R&D program pilots may be conditioned on country-of-origin disclosures, nationality vetting of key personnel, and source code control.

These factors are not always publicly articulated, but they are real gating items in practice, and companies must structure around them proactively.

Strategic structuring for market access

Given these gating items, foreign growth-stage companies must adopt a multi-prong approach to capitalize on the myriad opportunities presented by entering the U.S. market. These include:

(1) **U.S. subsidiary formation**: A well-structured U.S. subsidiary can reduce FOCI risk, isolate export controls, and position a company to receive federal funding. However, the company must be governed and capitalized with care. Ownership thresholds, information control policies, and voting rights all matter in government review.

(2) **Licensing and tech transfer**: For companies unwilling or unable to fully localize, structured technology license agreements with clear field-of-use restrictions, sublicensing controls, and audit rights can provide a compliant path to monetization while protecting enterprise value.

(3) **Controlled engagement pathways**: Teaming agreements with U.S.-based primes or Small and Medium-sized Enterprises (SMEs) allow companies to enter the federal supply chain without triggering standalone reviews. These agreements must address IP ownership, data rights (DFARS 252.227-7013/7015), and indemnity clauses that account for export and security law risks.

(4) **CFIUS-safe capital planning**: As investment becomes a vector for regulatory scrutiny, capital stack design should anticipate CFIUS exposure. Preferred structures include ring-fenced U.S. tranches, dual-class voting schemes, and options for converting SAFEs (Simple Agreement for Future Equity) or notes into non-voting equity.

(5) **Institutional readiness**: Whether applying for a grant or responding to a Broad Agency Announcement (BAA), companies should maintain compliance documentation — including export classification memos, cybersecurity attestations (NIST SP 800-171/CMMC), and governance policies for national security vetting.

In today's global technology order, national security is no longer a siloed legal discipline; it is the lens through which opportunity, access, and trust are evaluated. The companies that thrive in this landscape are not just innovative, they are structurally aligned and operationally trusted.

For foreign dual-use technology companies interested in doing business in the U.S., it is critical to engage legal counsel early. Counsel can help navigate corporate structuring, export controls, government contracts, and strategic transactions in ways that anticipate regulatory expectations, minimize disruption, and position the business for sustainable growth. Taking a proactive approach ensures that compliance is not just reactive but integrated into long-term strategy.

About the authors

Scott Nuzum, special counsel in **Wiley**'s corporate practice, advises clients at the intersection of corporate law, national security, and emerging technology, including corporate transactions, technology licensing, export controls, and CFIUS compliance. He is based in Washington, D.C., and can be reached at snuzum@wiley.law.

This article was first published on Reuters Legal News and Westlaw Today on October 3, 2025.